DATASHEET

WATCHGUARD EPDR

Rilevamento e risposta per la protezione degli endpoint

SFIDE CORRELATE ALLA SICUREZZA INFORMATICA PER LE ORGANIZZAZIONI

Con l'aumento della complessità dell'infrastruttura tecnologica, le organizzazioni stanno faticando a trovare le competenze e le risorse di cui hanno bisogno per monitorare e gestire i rischi connessi alla sicurezza degli endpoint, che rappresentano l'obiettivo principale della maggior parte degli attacchi informatici. Quali sfide affrontano le aziende quando cercano di adottare soluzioni di sicurezza degli endpoint?

- **Sovraccarico di alert:** le organizzazioni ricevono ogni settimana migliaia di alert relativi ai malware, di cui soltanto il 19% viene reputato affidabile, mentre solo il 4% diventa oggetto di ulteriori indagini. Due terzi del tempo degli amministratori della sicurezza informatica sono dedicati alla gestione degli alert relativi a malware.
- **Complessità:** i professionisti della sicurezza possono avere difficoltà a gestire un numero troppo elevato di strumenti di sicurezza informatica scollegati, a causa del numero di tecnologie usate, della mancanza di competenze in-house e del tempo necessario per identificare le minacce.
- **Prestazioni scadenti:** poiché spesso le soluzioni di sicurezza degli endpoint richiedono l'installazione e la gestione di più agenti su ogni computer, server e laptop monitorato, è possibile incorrere in errori gravi, prestazioni scadenti e consumo elevato di risorse.

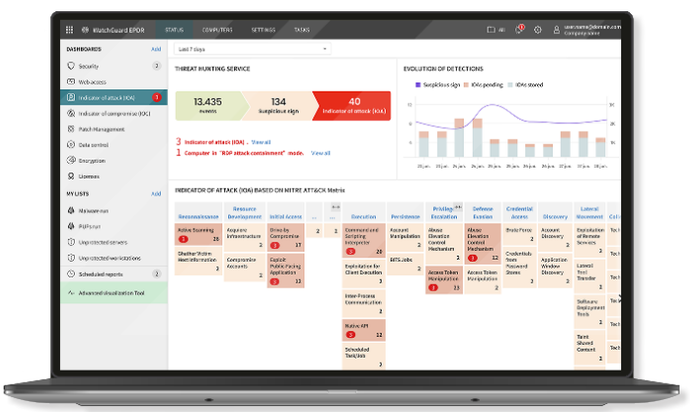
Le tecnologie di protezione degli endpoint tradizionali, incentrate sulla prevenzione, sono valide per le minacce note e i comportamenti dannosi, ma non sono sufficienti in caso di minacce informatiche avanzate. Dai vettori di compromissione più diffusi alle nuove minacce, gli autori degli attacchi sono sempre alla ricerca di nuovi modi per eludere le notifiche IT, sfuggire alle misure di difesa e sfruttare le vulnerabilità emergenti.

DALLA PREVENZIONE ALLA RISPOSTA - SICUREZZA DEGLI ENDPOINT AUTOMATIZZATA

WatchGuard EPDR è una soluzione cloud innovativa per la sicurezza informatica pensata per computer, laptop e server che automatizza la prevenzione, il rilevamento, il contenimento e la risposta a qualsiasi minaccia avanzata, dal malware zero day al ransomware, fino ai tentativi di phishing e agli exploit in memoria, compresi gli attacchi malwareless e fileless, sia all'interno che all'esterno della rete.

A differenza di altre soluzioni, unisce la più ampia gamma di tecnologie di protezione degli endpoint (EPP) con le funzionalità di rilevamento e risposta (EDR) automatizzate. Integra inoltre due servizi, gestiti dagli esperti di WatchGuard, che vengono erogati come una funzione della soluzione:

- **Servizio Zero Trust Application:** Classificazione al 100% delle applicazioni
- **Servizio di ricerca delle minacce:** rilevamento di hacker e utenti interni malevoli



WatchGuard EPDR integra in un'unica soluzione le tecnologie destinate agli endpoint tradizionali e le funzionalità innovative e adattive di protezione, rilevamento e risposta. I professionisti IT possono quindi affrontare le minacce informatiche avanzate ricorrendo alle tecnologie di sicurezza avanzate seguenti:

Tecnologie di prevenzione tradizionali

- Firewall personale o gestito (IDS)
- Controllo dispositivi
- Intelligenza collettiva
- Elenco non consentiti/Elenco consentiti
- Antimalware multivettoriale permanente e scansione on-demand
- Euristica pre-esecuzione
- Filtro degli URL e navigazione Web
- Antiphishing
- Antimanomissione
- Correzione e rollback

Tecnologie di sicurezza avanzate

- Monitoraggio continuo degli endpoint con EDR
- Apprendimento automatico basato su cloud che classifica il 100% dei processi (APT, ransomware, rootkit, ecc.)
- Sandboxing in ambienti reali
- Protezione anti-exploit
- Ricerca delle minacce, tra cui analisi comportamentale e rilevamento degli IoA (indicatori di attacco) per individuare gli attacchi Living off the Land (LotL)
- Indicatori di attacco collegati al MITRE ATT&CK Framework
- Rilevamento e prevenzione di attacchi RDP
- Funzionalità di contenimento e correzione, come isolamento del computer e blocco del programma tramite hash o nome

VANTAGGI

Semplificazione e ottimizzazione della sicurezza

- I servizi automatizzati riducono i costi del personale esperto. Non sono presenti falsi avvisi da gestire, non sono richieste lunghe impostazioni manuali e non viene delegata alcuna responsabilità.
- Non è necessario eseguire attività di installazione, configurazione o manutenzione delle infrastrutture di gestione.
- L'agente leggero e l'architettura nativa per il cloud non influiscono negativamente sulle prestazioni degli endpoint.

Facilità d'uso e di gestione

- Il portafoglio di sicurezza degli endpoint gestisce tutte le esigenze di protezione degli endpoint in modo straordinariamente semplice da un'unica console Web.
- L'installazione è semplice e Gestione degli endpoint tra più piattaforme da un unico pannello di controllo.
- dotato di un'interfaccia utente chiara e intuitiva.

Funzionalità EDR automatizzate

- Rileva e blocca le tecniche, le tattiche e le procedure di attacco, nonché l'attività dannosa in memoria (exploit) prima che possa diventare pericolosa.
- Risoluzione e risposta: analisi forense per indagare a fondo su ogni tentativo di attacco e strumenti per mitigarne gli effetti (disinfezione).
- Tracciabilità di tutte le azioni; visibilità pratica dell'aggressore e delle sue attività con la possibilità di intervenire direttamente, facilitando le indagini forensi.

MODELLO ZERO TRUST: PROTEZIONE MULTILIVELLO

La piattaforma di sicurezza degli endpoint di WatchGuard non si affida a una sola tecnologia, ma ricorre a più strumenti per ridurre le probabilità di successo degli autori delle minacce. Lavorando di concerto, queste tecnologie utilizzano le risorse in corrispondenza dell'endpoint per minimizzare il rischio di una violazione.

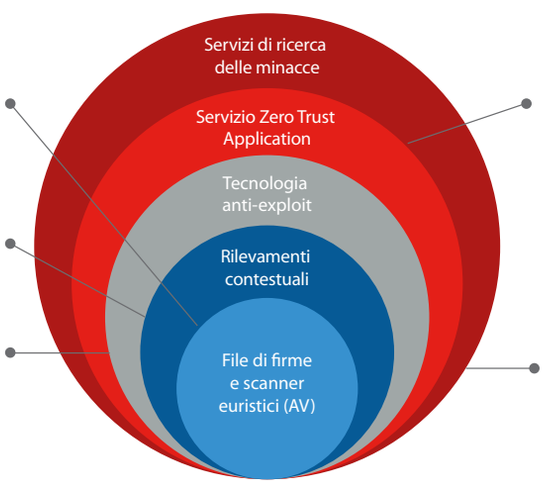
Modello Zero Trust: protezione multilivello

LIVELLI DEGLI ENDPOINT:

Livello 1/File di firma e tecnologie euristiche
Tecnologia efficace e ottimizzata per rilevare gli attacchi noti

Livello 2/Rilevamenti contestuali
Ci consentono di rilevare attacchi malwareless e fileless

Livello 3/Tecnologia anti-exploit
Ci consente di rilevare attacchi fileless progettati per sfruttare le vulnerabilità



LIVELLI NATIVI PER IL CLOUD

Livello 4/Servizio Zero Trust per le applicazioni
Offre funzionalità di rilevamento se si verifica una violazione in un livello precedente, interrompe gli attacchi su computer già infettati e interrompe gli attacchi basati su movimenti laterali all'interno della rete

Livello 5/Servizio di ricerca delle minacce
Ci consente di rilevare gli endpoint compromessi, gli attacchi in una fase iniziale, le attività sospette e il rilevamento di IoA

I file di firma e le tecnologie euristiche, conosciuti come protezione tradizionale degli endpoint (EPP), creano un livello di tecnologia antivirus di nuova generazione che si è dimostrato efficace contro numerose minacce comuni di basso livello. È ottimizzato per rilevare gli attacchi noti, sulla base di firme specifiche, rilevamento generico ed euristico e blocco degli URL malevoli.

Essenziale per il rilevamento di attacchi malwareless e senza file, il rilevamento contestuale cerca utilizzi anomali delle risorse e delle applicazioni. È molto efficace contro gli attacchi basati su script, gli attacchi che utilizzano strumenti legittimi del sistema operativo come PowerShell, WMI e così via, le vulnerabilità del browser Web e altre applicazioni che sono spesso prese di mira come Java, Adobe e altre ancora.

La tecnologia anti-exploit rileva gli attacchi fileless che sono progettati per sfruttare le vulnerabilità. Cerca e rileva comportamenti anomali, segnale sicuro di processi di exploit. La tecnologia anti-exploit è cruciale per gli endpoint che non sono più supportati e per gli endpoint con sistemi operativi non più supportati.

Il nostro **servizio Zero Trust Application** classifica il 100% dei processi, monitora l'attività degli endpoint e blocca l'esecuzione delle applicazioni e dei processi malevolii. Ogni esecuzione viene classificata in tempo reale come malevola o legittima senza incertezze e senza delegare le decisioni all'utente ed evitando i processi manuali.

Il **Servizio di ricerca delle minacce** si basa su una serie di regole create da esperti nel settore che vengono eseguite automaticamente a fronte di tutti i dati raccolti dalla telemetria, attivando indicatori di attacco estremamente attendibili e con un basso indice di falsi positivi, in modo da ridurre al minimo i tempi medi di rilevamento e risposta (Mean Time To Detect, MTTD e Mean Time To Respond, MTTR).

Piattaforme supportate e requisiti di sistema di WatchGuard EPDR

Sistemi operativi supportati: Windows (Intel e ARM), macOS (Intel e ARM), Linux e Android.

Supporto per sistemi esistenti a partire da Windows XP SP3 e Server 2003.

Le funzionalità EDR sono disponibili in Windows, macOS e Linux; Windows è la piattaforma che ne garantisce la piena operatività.

Elenco dei browser compatibili: Google Chrome, Mozilla Firefox, Internet Explorer, Microsoft Edge e Opera.

Numero verde Italia: 800.911.938 VENDITE INTERNAZIONALI: +1.206.613.0895 WEB: www.watchguard.com/it WatchGuard Technologies, Inc.